Amendments to the Claims

Claim 1 (currently amended): A computer program product for enabling an identity change during a certificate-based host access session, said computer program product embodied on a computer-readable medium and comprising:

computer-readable program code means for processing a first sign-on during a secure session using a digital certificate, further comprising:

computer-readable program code means for establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

computer-readable program code means for storing said digital certificate or a reference thereto at said server machine;

computer-readable program code means for establishing a session from said server machine to a host system using a legacy host communication protocol, responsive to receiving, at said server machine, a first sign-on request from said client machine, wherein said first sign-on request identifies a first secure legacy host application to which said first sign-on is requested;

computer-readable program code means for passing said stored digital certificate or said reference from said server machine to a host access security system;

computer-readable program code means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

computer-readable program code means, operable in said host access security system, for using said passed or retrieved digital certificate to locate access credentials for said

user;

computer-readable program code means, operable in said host access security system, for accessing a stored password or generating a password substitute representing said located credentials;

computer-readable program code means, operable in said host access security system, for returning said stored password or generated password substitute to said server machine, along with a first user identifier corresponding to said located credentials;

computer-readable program code means for requesting by said first secure legacy host application, responsive to said computer-readable program code means for establishing said session, first sign-on information for said user; and

computer-readable program code means for responding to said request for first sign-on information by sending a first sign-on message with placeholder syntax from said client machine to said server machine, said placeholder syntax representing a user identification and a password of said user, wherein said user identification and said password are expected in said first sign-on message by said first secure legacy host application; and

computer-readable program code means, operable in said server machine, for using said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on, on behalf of said user of said client machine, to said first secure legacy host application executing at said host system by substituting said returned first user identifier and said returned password or password substitute for said placeholder syntax in said first sign-on message, thereby creating a revised first sign-on message, and forwarding said revised first sign-on message from said server machine to said first secure legacy host application;

and

computer-readable program code means for processing a second sign-on during said secure session, without requiring establishment of a new secure session between said client machine and said server machine, using a second digital certificate that represents a second identity, further comprising:

computer-readable program code means for receiving a second sign-on request, at said server machine from said client machine, wherein: (1) said second sign-on request identifies a second secure legacy host application to which said second sign-on is requested; (2) said second sign-on request includes said second digital certificate, or a second certificate reference that references said second digital certificate, for said second identity; (3) said second secure legacy host application may be identical to said first secure legacy host application; and (4) said second identity is for a second user, wherein said second user may be identical to said user;

computer-readable program code means for passing said second digital certificate or said second certificate reference from said server machine to said host access security system;

computer-readable program code means, operable in said host access security system, for authenticating said second identity using said passed second digital certificate or a second retrieved certificate which is retrieved using said second certificate reference;

computer-readable program code means, operable in said host access security system, for using said passed second digital certificate or said second retrieved certificate to locate second access credentials for said second user;

computer-readable program code means, operable in said host access security system, for accessing a second stored password or generating a second password substitute

representing said second located credentials;

computer-readable program code means, operable in said host access security system, for returning said second stored password or second generated password substitute to said server machine, along with a second user identifier corresponding to said second located credentials; and

computer-readable program code means, operable in said server machine, for using said returned second password or second password substitute and said returned second user identifier to transparently complete said second sign-on, on behalf of said second user of said client machine, to said second secure legacy host application executing at said host system.

Claim 2 (previously presented): The computer program product as claimed in Claim 1, wherein said digital certificate and said second digital certificate are X.509 certificates and said digital certificate reference and second certificate reference are references to an X.509 certificate.

Claim 3 (original): The computer program product as claimed in Claim 1, wherein said communication protocol is a 3270 emulation protocol.

Claim 4 (original): The computer program product as claimed in Claim 1, wherein said communication protocol is a 5250 emulation protocol.

Claim 5 (original): The computer program product as claimed in Claim 1, wherein said communication protocol is a Virtual Terminal protocol.

Claim 6 (original): The computer program product as claimed in Claim 3, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 7 (previously presented): The computer program product as claimed in Claim 1, wherein said computer-readable program code means for processing said second sign-on further comprises computer-readable program code means for storing said second digital certificate at said server machine.

Claim 8 (canceled)

Claim 9 (currently amended): A system for enabling an identity change during a certificate-based host access session, comprising:

means for processing a first sign-on during a secure session using a digital certificate, further comprising:

means for establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

means for storing said digital certificate or a reference thereto at said server machine;

means for establishing a session from said server machine to a host system using a legacy host communication protocol, responsive to receiving, at said server machine, a first sign-

on request from said client machine, wherein said first sign-on request identifies a first secure legacy host application to which said first sign-on is requested;

means for passing said stored digital certificate or said reference from said server machine to a host access security system;

means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

means, operable in said host access security system, for using said passed or retrieved digital certificate to locate access credentials for said user;

means, operable in said host access security system, for accessing a stored password or generating a password substitute representing said located credentials;

means, operable in said host access security system, for returning said stored password or generated password substitute to said server machine, along with a first user identifier corresponding to said located credentials;

means for requesting by said first secure legacy host application, responsive to said computer-readable program code means for establishing said session, first sign-on information for said user; and

means for responding to said request for first sign-on information by sending a first sign-on message with placeholder syntax from said client machine to said server machine, said placeholder syntax representing a user identification and a password of said user, wherein said user identification and said password are expected in said first sign-on message by said first secure legacy host application; and

means, operable in said server machine, for using said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on, on behalf of said user of said client machine, to said first secure legacy host application executing at said host system by substituting said returned first user identifier and said returned password or password substitute for said placeholder syntax in said first sign-on message, thereby creating a revised first sign-on message, and forwarding said revised first sign-on message from said server machine to said first secure legacy host application;; and

means for processing a second sign-on during said secure session, without requiring establishment of a new secure session between said client machine and said server machine, using a second digital certificate that represents a second identity, further comprising:

means for receiving a second sign-on request, at said server machine from said client machine, wherein: (1) said second sign-on request identifies a second secure legacy host application to which said second sign-on is requested; (2) said second sign-on request includes said second digital certificate, or a second certificate reference that references said second digital certificate, for said second identity; (3) said second secure legacy host application may be identical to said first secure legacy host application; and (4) said second identity is for a second user, wherein said second user may be identical to said user;

means for passing said second digital certificate or said second certificate reference from said server machine to said host access security system;

means, operable in said host access security system, for authenticating said second identity using said passed second digital certificate or a second retrieved certificate which is retrieved using said second certificate reference;

means, operable in said host access security system, for using said passed second digital certificate or said second retrieved certificate to locate second access credentials for said second user;

means, operable in said host access security system, for accessing a second stored password or generating a second password substitute representing said second located credentials;

means, operable in said host access security system, for returning said second stored password or second generated password substitute to said server machine, along with a second user identifier corresponding to said second located credentials; and

means, operable in said server machine, for using said returned second password or second password substitute and said returned second user identifier to transparently complete said second sign-on, on behalf of said second user of said client machine, to said second secure legacy host application executing at said host system.

Claim 10 (previously presented): The system as claimed in Claim 9, wherein said digital certificate and said second digital certificate are X.509 certificates and said digital certificate reference and second certificate reference are references to an X.509 certificate.

Claim 11 (original): The system as claimed in Claim 9, wherein said communication protocol is a 3270 emulation protocol.

Claim 12 (original): The system as claimed in Claim 11, wherein said host access security system

is a Resource Access Control Facility (RACF) system.

Claim 13 (previously presented): The system as claimed in Claim 9, wherein said means for processing said second sign-on further comprises means for storing said second digital certificate at said server machine.

Claim 14 (canceled)

Claim 15 (currently amended): A method for enabling an identity change during a certificate-based host access session, comprising the steps of:

processing a first sign-on during a secure session using a digital certificate, further comprising the steps of:

establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

storing said digital certificate or a reference thereto at said server machine;

establishing a session from said server machine to a host system using a legacy host communication protocol, responsive to receiving, at said server machine, a first sign-on request from said client machine, wherein said first sign-on request identifies a first secure legacy host application to which said first sign-on is requested;

passing said stored digital certificate or said reference from said server machine to a host access security system;

authenticating, by said host access security system, said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

using, by said host access security system, said passed or retrieved digital certificate to locate access credentials for said user;

accessing, by said host access security system, a stored password or generating a password substitute representing said located credentials;

returning, by said host access security system, said stored password or generated password substitute to said server machine, along with a first user identifier corresponding to said located credentials;

requesting by said first secure legacy host application, responsive to said computer-readable program code means for establishing said session, first sign-on information for said user; and

responding to said request for first sign-on information by sending a first sign-on message with placeholder syntax from said client machine to said server machine, said placeholder syntax representing a user identification and a password of said user, wherein said user identification and said password are expected in said first sign-on message by said first secure legacy host application; and

using, by said server machine, said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on, on behalf of said user of said client machine, to said first secure legacy host application executing at said host system by substituting said returned first user identifier and said returned password or password substitute for said placeholder syntax in said first sign-on message, thereby creating a revised first sign-on

message, and forwarding said revised first sign-on message from said server machine to said first secure legacy host application;; and

processing a second sign-on during said secure session, without requiring establishment of a new secure session between said client machine and said server machine, using a second digital certificate that represents a second identity, further comprising the steps of:

receiving a second sign-on request, at said server machine from said client machine, wherein: (1) said second sign-on request identifies a second secure legacy host application to which said second sign-on is requested; (2) said second sign-on request includes said second digital certificate, or a second certificate reference that references said second digital certificate, for said second identity; (3) said second secure legacy host application may be identical to said first secure legacy host application; and (4) said second identity is for a second user, wherein said second user may be identical to said user;

passing said second digital certificate or said second certificate reference from said server machine to said host access security system;

authenticating, by said host access security system, said second identity using said passed second digital certificate or a second retrieved certificate which is retrieved using said second certificate reference;

using, by said host access security system, said passed second digital certificate or said second retrieved certificate to locate second access credentials for said second user;

accessing, by said host access security system, a second stored password or generating a second password substitute representing said second located credentials;

returning, by said host access security system, said second stored password or

second generated password substitute to said server machine, along with a second identifier corresponding to said second located credentials; and

using, by said server machine, said returned second password or second password substitute and said returned second user identifier to transparently complete said second sign-on, on behalf of said second user of said client machine, to said second secure legacy host application executing at said host system.

Claim 16 (previously presented): The method as claimed in Claim 15, wherein said digital certificate and said second digital certificate are X.509 certificates and said digital certificate reference and second certificate reference are references to an X.509 certificate.

Claim 17 (original): The method as claimed in Claim 15, wherein said communication protocol is a 3270 emulation protocol.

Claim 18 (original): The method as claimed in Claim 17, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 19 (previously presented): The method as claimed in Claim 15, wherein said step of processing said second sign-on further comprises the step of storing said second digital certificate at said server machine.

Claim 20 (canceled)

Claim 21 (currently amended): The computer program product as claimed in Claim 1, wherein:

said computer-readable program code means for processing said second sign-on further comprises computer-readable program code means for receiving, at said server machine, a second sign-on message sent from said client machine, wherein said second sign-on message has ~~placeholders~~ placeholder syntax representing a user identification of said second user and a password of said second user, wherein said user identification of said second user and said password of said second user are expected in said second sign-on message by said second secure legacy host application; and

said computer-readable program code means for using said returned second password or second password substitute and said returned second user identifier to transparently complete said second sign-on further comprises:

computer-readable program code means for substituting said returned second user identifier and said returned second password or second password substitute for said ~~placeholders~~ placeholder syntax in said second sign-on message, thereby creating a revised second sign-on message; and

computer-readable program code means for forwarding said revised second sign-on message from said server machine to said second secure legacy host application.

Claim 22 (previously presented): The computer program product according to Claim 1, wherein said second sign-on request includes information usable as proof that said second user owns said second digital certificate.

Claim 23 (previously presented): The computer program product according to Claim 22, wherein said proof further comprises a random seed value and a sequence number concatenated thereto by said client machine to detect replay attacks, wherein said random seed value was previously sent from said server machine to said client machine.

Claim 24 (previously presented): The computer program product according to Claim 23, wherein said identification of said second secure legacy host application is also concatenated to said random seed value.

Claim 25 (previously presented): The computer program product according to Claim 23, wherein a digital signature computed using a private key associated with said second digital certificate is included in said second sign-on request, said digital signature covering said random seed value and said concatenated sequence number.

Claim 26 (previously presented): The computer program product according to Claim 24, wherein a digital signature computed using a private key associated with said second digital certificate is included in said second sign-on request, said digital signature covering said random seed value, said concatenated sequence number, and said concatenated identification of said second secure legacy host application.

Claim 27 (currently amended): The system as claimed in Claim 9, wherein:

said means for processing said second sign-on further comprises means for receiving, at said server machine, a second sign-on message sent from said client machine, wherein said second sign-on message has ~~placeholders~~ placeholder syntax representing a user identification of said second user and a password of said second user, wherein said user identification of said second user and said password of said second user are expected in said second sign-on message by said second secure legacy host application; and

said means for using said returned second password or second password substitute and said returned second user identifier to transparently complete said second sign-on further comprises:

means for substituting said returned second user identifier and said returned second password or second password substitute for said ~~placeholders~~ placeholder syntax in said second sign-on message, thereby creating a revised second sign-on message; and

means for forwarding said revised second sign-on message from said server machine to said second secure legacy host application.

Claim 28 (currently amended): The method as claimed in Claim 15, wherein:

said step of processing said second sign-on further comprises the step of receiving, at said server machine, a second sign-on message sent from said client machine, wherein said second sign-on message has ~~placeholders~~ placeholder syntax representing a user identification of said second user and a password of said second user, wherein said user identification of said second user and said password of said second user are expected in said second sign-on message by said second secure legacy host application; and

said step of using said returned second password or second password substitute and said returned second user identifier to transparently complete said second sign-on further comprises the steps of:

substituting said returned second user identifier and said returned second password or second password substitute for said ~~placeholders~~ placeholder syntax in said second sign-on message, thereby creating a revised second sign-on message; and

forwarding said revised second sign-on message from said server machine to said second secure legacy host application.

Claim 29 (currently amended): A computer-implemented method for enabling an identity change during a certificate-based host access session, comprising steps of:

establishing a secure session between a client and a server using a digital certificate owned by a user of said client;

remembering said digital certificate at said server;

completing a first sign-on to a host application, by said server on behalf of said user, responsive to receiving an asynchronous sign-on request from said client that identifies said host application, further comprising the steps of:

using said remembered digital certificate to authenticate said user to a host access security component;

if said user is authenticated, locating, by said host access security component, access credentials of said user;

creating, by said host access security component, a passticket that represents said

located access credentials;

returning said passticket from said host access security component to said server, along with a user identifier associated with said located access credentials; and

inserting, by said server, said passticket and said user identifier into a log-on message in place of placeholders ~~therefor~~ for a user password and said user identifier, when said log-on message is received at said server from said client, thereby creating a revised log-on message, in a form expected by said host application, that is then sent from said server to sign said user on to said host application; and

completing a second sign-on to a second host application, by said server on behalf of a second user, responsive to receiving a second asynchronous sign-on request from said client that identifies said second host application, wherein said second host application may be identical to said host application and said second user may be identical to said user, further comprising the steps of:

using a new digital certificate and proof therefor to authenticate said second user to said host access security component, wherein said new digital certificate and said proof therefor are included in said second asynchronous sign-on request;

if said second user is authenticated, locating, by said host access security component, access credentials of said second user;

creating, by said host access security component, a second passticket that represents said located access credentials of said second user;

returning said second passticket from said host access security component to said server, along with a second user identifier associated with said located access credentials of said

second user; and

inserting, by said server, said returned second passticket and said returned second user identifier into a second log-on message in place of placeholders ~~therefor~~ for a second user password and said second user identifier, when said second log-on message is received at said server from said client, thereby creating a revised second log-on message, in said form expected by said second host application, that is then sent from said server to sign said second user on to said second host application.

Claim 30 (new): A method of providing identity change during a secure session, comprising steps of:

upon receiving a first log-on message containing placeholder syntax from a client during a secure session, substituting therefor a first user identifier and a first password substitute provided by a host access security system upon authentication of user credentials associated with the client and with a user thereof, thereby creating a revised first log-on message in a form expected by a first legacy host application, the first password substitute representing access privileges associated with the user credentials for the first legacy host application;

forwarding the revised first log-on message to the first legacy host application for completing a secure sign-on thereto;

upon receiving a second log-on message containing placeholder syntax from the client during the secure session, substituting therefor a second user identifier and a second password substitute provided by the host access security system upon authentication of second user credentials associated with the client and with the user thereof or a different user thereof, thereby

creating a revised second log-on message in a form expected by a second legacy host application, the second password substitute representing access privileges associated with the second user credentials for the second legacy host application, wherein the second legacy host application may be identical to the first legacy host application; and

forwarding the revised second log-on message to the second legacy host application for completing a secure sign-on thereto.